

INFORMATION TECHNOLOGY POLICY

For consideration May 2026

Introduction	2
Purpose of the IT Policy	2
Monitoring of IT use	2
Scope of this policy	2
Computer use	2
Equipment	3
Health and safety	5
Password and authentication policy	5
Monitoring	6
Remote working	7
Email	8
Use of the internet	8
Use of social media	9
Misuse	11
Important notice	11

Introduction

Each council will have its own IT setup and, as such, a single 'one-size-fits-all' IT policy is unlikely to be appropriate. Some smaller parish councils may operate with minimal equipment, while others may manage multiple devices connected to a central server. These guidelines are intended to help councils identify key considerations when developing or updating their own IT policy.

Councils that use external IT providers should ensure their policies accurately reflect current practices and contractual arrangements.

Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors, staff, and other authorised users use council-provided technology or equipment in the course of their duties. A well-defined policy helps to:

- Set expectations for appropriate use of equipment and systems;
- Raise awareness of risks associated with IT use;
- Safeguard the council's data and digital assets;
- Clarify what constitutes acceptable and unacceptable use;
- Outline the consequences of policy breaches.

Councils will also need to determine and clearly state whether limited personal use of IT equipment is permitted (for example, checking personal email or online shopping during lunch breaks).

Monitoring of IT Use

As an IT provider, the council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and councillors, employees and other authorised users are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws. Other persons may be included if they access or use council systems e.g. if they have a council e-mail address

Scope of this policy

This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, including those who are home-based, office-based or work on a flexible or part-time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

1. Computer use

1.1.1 If council computer equipment is provided for council purposes, reasonable personal use is permitted ('reasonable' interpreted as in the opinion of the council) and should not interrupt daily council work in any way. Councillors, staff and other authorised users are asked to restrict any personal use to official break times and outside working hours.

1.1.2 All councillors, staff and other authorised users must lock their computers when unattended to prevent unauthorised access. This applies to all council and personal devices used for work. Failure to comply may lead to disciplinary action.

1.1.3 Any damage sustained to council-owned equipment will have a financial impact on the council and equipment should be treated with care.

1.1.4 Council-owned computer and electronic hardware should be kept clean and every precaution taken to prevent food and drink being dropped or spilled onto it.

1.1.5 Equipment should not be dismantled or reassembled without seeking advice.

1.1.6 Councillors, staff and other authorised users are not to purchase any computer or mobile equipment (including software) for the council, unless previously authorised.

1.1.7 Personal discs, USB drives or devices, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the council.

2. Equipment

2.1 Portable equipment

2.1.1 Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

2.1.2 It is particularly emphasised that council back-up procedures specific to portable equipment should be followed at all times.

2.1.3 All portable computers must be stored safely and securely when not in use. Portable equipment should be kept with or near the user when away from the premises and should never be left in parked vehicles.

2.1.4 It is important to ensure that all portable devices are protected with encryption in case they are lost or stolen. All smartphones or tablets that hold council data, including emails and files, must be protected with a pin code. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disabled or removed.

2.1.5 Multi-Factor Authentication (MFA) is a security process that requires users to verify their identity using two or more independent methods—for example, entering a password (something you know) and confirming a code sent to your mobile device (something you have). This significantly reduces the risk of unauthorised access to systems and sensitive data. NALC recommends implementing MFA as a best practice to enhance information security and support compliance with data protection obligations under the UK GDPR and the Data Protection Act 2018.

2.1.6 If an item of portable equipment is lost or damaged this should be reported to the clerk. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the cost of the loss/damage.

2.1.7 Under no circumstances should any non public meeting or conversation be recorded without the permission of those present. This does not affect statutory rights under The Openness of Local Government Regulations 2014.

2.1.8 In addition, the council does not permit webcams (which may be pre-installed on many laptops) to be used in the workplace, other than for conference calls for council purposes. If there is any doubt as to whether a device falls under this clause, advice should be sought from the clerk.

2.2 Use of own devices

2.2.1 The Council recognises that some councillors, staff, and other authorised users may wish to use their own smartphones, tablets, laptops etc to access servers, private clouds or networks for normal council purposes, including, but not limited to, reading email, accessing documents stored on the council's shared drive or to store data on the council's shared drive or access data in other services. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux - in commercial configurations) will normally be permitted. Such devices

should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

2.2.2 However, the same security precautions apply to personal devices as to the council's desktop equipment. If calls are made from personal phones to external parties, ensure that personal numbers and data are not shared by councillors and staff. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

2.2.3 Councillors, staff, and other authorised persons that use council systems are expected to use all devices in an ethical and respectful manner and in accordance with this policy. Accessing inappropriate websites or services on any device via the IT infrastructure that is paid for or provided by the council carries a high degree of risk and for employees, may result in disciplinary action, including summary dismissal (without notice). For workers or contractors, we may terminate the worker agreement. This is irrespective of the ownership of the device used. An example would be downloading copyright music illegally or accessing pornographic material.

2.2.4 In cases of legal proceedings against the council, the council may need to temporarily take possession of a device, whether council-owned or personal, to retrieve the relevant data.

2.2.5 Wherever possible the user should maintain a clear separation between the personal data processed on the council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

2.2.6 Councillors, staff and other authorised users who intend to use their own devices via the council's infrastructure must ensure that they:

- use a 6-digit pin, strong password or finger print (preferably the latter) to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after 4 failed login attempts;
- configure their device(s) to automatically prompt for a password after a period of inactivity of more than 10 minutes;
- always password protect any documents containing confidential information that are sent as attachments to an email and notify the password separately (preferably by a means other than email);
- for smartphones and tablets, activate the automatic device wipe function (where available). Note that use of the remote wipe function may also involve the removal of the individual's personal data. Councillors, staff, and other authorised users are therefore advised to keep personal data separate from council data where possible;
- ensure secure WiFi networks are used;
- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device;
- Inform the clerk if their device(s) is/are lost, stolen or inappropriately accessed where there is risk of access to council data or resources. To prevent phones being used, they will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

2.2.7 Any work done on user's own equipment should be stored securely and password protected and should always be backed up in accordance with the council's standard backup procedures.

2.2.8 Prior to the disposal of any device that has work data stored on it, and in the event of a user leaving the council, councillors, staff, and other authorised users are

required to allow the clerk access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

2.2.9 Councillors, staff and other authorised users must take responsibility for understanding how their device(s) work in respect to the above rules if they are accessing council servers/services via their own IT equipment. Risks to the user's personal device(s) include data loss as a result of a crash of the operating system, bugs and viruses, software or hardware failures and programming errors rendering a device inoperable. The council will use reasonable endeavours to assist, but councillors, staff and other authorised users are personally liable for their own device(s) and for any costs incurred as a result of the above.

3. Health and safety

3.1.1 The council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment. This should be claimed back as an employee expense.

3.1.2 Any VDU user who feels that their workstation requires changes to make it compliant must speak to the staffing committee.

3.1.3 If any hazards are detected at a workstation, including 'noises' from council-owned IT equipment, this should be reported immediately to the clerk.

4. Password and Authentication Policy

4.1 Passwords

4.1.1 All user accounts must be protected by strong, secure passwords. The council follows the National Cyber Security Centre (NCSC) recommendations for creating passwords using three random words (e.g. PurpleCandleRiver). This method helps create passwords that are both strong and easy to remember, while offering effective protection against common cyber threats such as brute-force attacks. This approach is endorsed in NALC guidance.

4.1.2 To further strengthen account security:

- Initial user account passwords must be generated by the IT provider.
- Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
- Service or System (e.g. website) account passwords are generated and managed by the IT provider.

4.1.3 Access to Passwords:

- Passwords are personal and must not be shared under any circumstances.
- Only the assigned user of an account may access or use the associated password.
- In exceptional cases (e.g., incident response or employee offboarding), access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the clerk, in a sealed envelope, only to be accessed in an emergency.

4.1.4 Password Storage and Management:

- Passwords must not be stored in plain text or written down in insecure locations.

- Passwords must be stored using a council-approved, encrypted password manager (eg LastPass, Bitwarden or KeePass).

4.1.5 Password Change Requirements:

- Immediately change password if compromise is suspected.

4.1.6 Password Access Control and Logging:

- All access to administrative or shared credentials must be logged and auditable.
- Attempts to access unauthorised passwords will be treated as a security incident.

4.2 Authentication

4.2.1 Multi-Factor Authentication (MFA) should be enabled wherever possible. MFA requires users to provide two or more independent forms of verification—for example, a password (something you know) and a code sent to your phone (something you have). This significantly reduces the risk of unauthorised access to systems and personal data.

- The council recommends these practices as part of its commitment to robust information security and to support compliance with the UK GDPR and the Data Protection Act 2018.
- For more guidance, see the NCSC's advice on password security: [NCSC Password Guidance](#)

4.3 Responsibility

4.3.1 Users are responsible for creating and maintaining secure passwords for their accounts.

4.3.2 The IT security provider is responsible for:

- Managing system/service credentials.
- Enforcing password policies.
- Auditing and monitoring password-related security practices.

5. **Monitoring**

5.1.1 The council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage is continually monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

5.1.2 The council will monitor the use of electronic communications and use of the internet in line with the Investigatory Powers (Interception by Councils etc for Monitoring and Record-keeping Purposes) Regulations 2018.

5.1.3 Monitoring of an employee's email and/or internet use will be conducted in accordance with an impact assessment that the council has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the council's legitimate interests and is to ensure that this policy is being complied with.

5.1.4 The information obtained through monitoring may be shared internally, including with relevant councillors and IT staff if access to the data is necessary for performance of their roles. The information may also be shared with external HR or legal advisers for the purposes of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place.

5.1.5 The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

5.1.6 Councillors, staff, and other authorised users have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in the council's data protection policy.

5.1.7 Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

5.1.8 The council reserves the right to inspect all files stored on its computer systems in order to assure compliance with this policy. The council also reserves the right to monitor the types of sites being accessed and the extent and frequency of use of the internet at any time, both inside and outside of working hours to ensure that the system is not being abused and to protect the council from potential damage or disrepute.

5.1.9 Any use that the council considers to be 'improper', either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.

5.1.10 All computers will be periodically checked and scanned for unauthorised programmes and viruses.

6. Remote working

6.1.1 Increased IT security measures apply to those who work from home or away from their normal place of work, as follows:

- if logging into the council's systems or services remotely, using computers that either do not belong to the council or are not owned by the user, any passwords must not be saved, and the user must log out at the end of the session deleting all logs and history records within the browser used. If the configuration of the device does not clearly support these actions (for example at an internet café), council services should not be accessed from that device;
- the location and direction of the screen should be checked to ensure confidential information is out of view. Steps should be taken to avoid messages being read by other people, including other travellers on public transport etc;
- any data printed should be collected and stored securely;
- all electronic files should be password protected and the data saved to the council's system/services when accessible;
- papers, files or computer equipment must not be left unattended unless arrangements have been made with a responsible person at the premises for them to be kept in a locked room or cabinet if they are to be left unattended at any time;
- any data should be kept safely and should only be disposed of securely;
- papers, files, data sticks/storage, flash drive or backup hard drives should not be left unattended in cars, except where it is entirely unavoidable for short periods, in which case they must be locked in the boot of the car. If staying away overnight, council data should be taken into the accommodation, care being taken that it will not be interfered with by others or inadvertently destroyed;
- where possible the ability to remotely wipe any mobile devices that process sensitive information should be retained in the case of loss or theft.

6.1.2 Those issued with a 'dongle' to enable internet access from a laptop via 3G or 4G networks whilst away from their normal workplace should note that the cost of internet

access can be very high. Dongles should therefore be used for essential council purposes only, especially if abroad.

6.1.3 Similarly, use of paid for Wi-Fi access, for example at airports should be carefully monitored and restricted to essential council use.

7. Email

7.1.1 Council email facilities are intended to promote effective and speedy communication on work-related matters. Although email use is encouraged, it can be risky. Councillors, staff, and other authorised users need to be careful not to introduce viruses onto council systems and should take proper account of the security advice below.

7.1.2 It is often quicker to action an issue by telephone or face to face, rather than via protracted email chains. Emails should not be used as a substitute for face to face or telephone conversations. Councillors, staff, and other authorised users are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

7.1.3 These rules are designed to minimise the legal risks run when using email at work and to guide councillors, staff, and other authorised users as to what may and may not be done. If there is something which is not covered in the policy, councillors, staff, and other authorised users should ask the clerk, rather than assuming they know the right answer.

7.1.4 All councillors, staff, and other authorised users who need to use email as part of their role will normally be given their own council email address and account. The council may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or that the system is being abused.

7.1.5 Email messages sent on the council's account should be for council use only. Personal communications are permitted provided they do not encroach upon working time or interrupt council business in any way. Employees and other authorised users are asked to restrict their personal use to official breaks or outside working hours, and to use their personal email accounts, rather than council addresses.

8. Use of the Internet

8.1 Copyright

8.1.1 Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 sets out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the council and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.

8.1.2 It is easy to copy electronically, but this does not make it any less an offence. The council's policy is to comply with copyright laws, and not to bend the rules in any way.

8.1.3 Councillors, staff, and other authorised users should not assume that because a document or file is on the Internet, it can be freely copied. There is a difference between information in the 'public domain' (which is no longer confidential or secret information but is still copyright protected) and information which is not protected by copyright (such as where the author has been dead for more than 70 years).

8.1.4 Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

8.1.5 Copyright and database right law can be complicated. Councillors, staff, and other authorised users should check with the clerk if unsure about anything.

8.2 Trademarks, links and data protection

8.2.2 The council does not permit the registration of any new domain names or trademarks relating to the council's names or products anywhere in the world, unless authorised to do so. Nor should they add links from any of the council's web pages to any other external sites without checking first with the clerk.

8.2.3 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection policy on its website at westmillpc.org.uk/documentation

8.3 Accuracy of information

8.3.1 One of the main benefits of the internet is the access it gives to large amounts of information, which is often more up to date than traditional sources such as libraries. Be aware that, as the internet is uncontrolled, much of the information may be less accurate than it appears.

9. **Use of social media**

9.1.1 Social media includes; blogs; Wikipedia and other similar sites where text can be posted; multimedia or user generated media sites (YouTube); social networking sites such as WhatsApp, Facebook, LinkedIn, X, Instagram etc.); text messaging and mobile device communications; virtual worlds (Second Life); and more traditional forms of media such as TV and newspapers. Care should be taken when using social media at any time, either using council systems or at home.

9.1.2 Personal use of social networking/media and chat sites should be restricted to breaks during working hours or outside working hours.

9.1.3 The council recognises the importance of councillors, staff, and other authorised users joining in and helping to shape sector conversation and enhancing its image through blogging and interaction in social media such as WhatsApp or Facebook for example. Therefore, where it is relevant to use social networking sites as part of the individual's position, this is acceptable.

However, inappropriate comments and postings can adversely affect the reputation of the council, even if it is not directly referenced. If comments or photographs could reasonably be interpreted as being associated with the council, or if remarks could be regarded as abusive, humiliating, sexual harassment, discriminatory or derogatory, or could constitute bullying or harassment, the council will treat this as a serious disciplinary offence. Councillors, staff and other authorised users should be aware that residents or other local organisations may read councillors, staff and other authorised users' personal weblogs to acquire information, for example, about their work, internal council business and employee morale. Therefore, even if the council is not named, care should be taken with any views expressed.

9.1.4 To protect both the council and its interests, everyone is required to comply with the following rules about social media, whether in relation to their council role or personal social networking sites and irrespective of whether this is during or after working hours:

- Contacts from any of the council's databases should not be downloaded and connected with on LinkedIn, WhatsApp or other social networking sites with electronic address book facilities, unless this has been authorised.
- Any blog that mentions the council, its current work, councillors, employees, other users associated with the council, partner organisations, local groups, suppliers, electors, should identify the author as one of its councillors or employees and state that the views expressed on the blog or website are theirs alone and do not represent the views of the council. Even if the council is not mentioned, care should be taken with any views expressed on social media sites such as WhatsApp and any views should clearly be stated as the writer's own (eg via a disclaimer statement such as: "The comments and other content on this site are my own and do not represent the positions or opinions of the council"). Writers must not claim or give the impression that they are speaking on behalf of the council.
- Any employee who is developing a site or writing a blog that will mention the council, must inform the council that they are writing this and gain agreement before going 'live'.
- The council expects councillors, staff, and other authorised users to be respectful about the council and its current or potential staff, councillors, clerks and authorised users and not to engage in any name calling or any behaviour that will reflect negatively on its reputation. Any unauthorised use of copyright materials, any unfounded or derogatory statements or any misrepresentation could constitute gross misconduct.
- Photos or videos that include employees or other workers wearing uniforms or clothing displaying the council's name or logo should not be posted on social media if it could reflect negatively on the individual, their role, their colleagues or the council. Additionally, photos, videos or audio recordings must not be taken on council premises without explicit permission
- Comments posted by councillors, staff and other authorised users on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.
- Inappropriate conversations should not take place on any social networking sites such as WhatsApp or Facebook, including forums.
- Any writing about or displaying photos or videos of internal activities that involves current councillors, staff and other authorised persons, might be considered a breach of data protection and a breach of privacy and confidentiality. Therefore, their permission should be gained prior to uploading any such material. Details of any kind relating to any events, conversations, materials or documents that are meant to be private, confidential or internal to the council should not be posted. This may include manuals; procedures; training documents; non-public financial or operational information; personal information regarding other councillors, staff and other authorised users; anything to do with a disciplinary case, grievance, allegation of bullying/harassment or discrimination or legal issue; any other secret, confidential or proprietary information; or information that is subject to confidentiality agreements. This does not affect statutory requirements to publish information including under the Freedom of Information Act.
- Councillors, staff and other authorised users must be aware that they are personally liable for anything that they write or present online (including on an online forum or blog, post, feed or website). Councillors should always be mindful of the Members Code of Conduct and Nolan Principles. Employees may be subject to disciplinary action for comments, content, or images that are defamatory, embarrassing, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment. They may also be sued by other organisations, and any individual or council that views their comments, content or images as; defamatory; pornographic; proprietary; harassing; libellous; or creating a hostile work environment. In addition, other councillors, staff and other authorised users can raise grievances for alleged bullying and/or harassment.

- Postings to websites or anywhere on the internet and social media of any kind, or in any press or media of any kind, should not breach copyright or other law or disclose confidential information, defame or make derogatory comments about the council, its councillors or staff, or disclose personal data or information about any individual that could breach data protection legislation.
- Contacts by the media relating to the council, should be referred to the clerk.
- Councillors, staff, and other authorised users who use sites such as LinkedIn and Facebook must ensure that the information on their profile is accurate and up to date and must update their profile on leaving the council.
- Councillors, staff, and other authorised users who use X.com, LinkedIn, or other social media/networking sites for council development purposes must ensure they provide the council with login details, including password(s), so that these sites can be accessed and updated in their absence.
- Councillors, staff, and other authorised users who have left the council must not post any inappropriate comments about the council or its councillors, staff and other authorised users on WhatsApp, LinkedIn, Facebook, X.com or any other social media/networking sites.
- During your employment/ involvement with the council, you may create or obtain access to a variety of professional contacts and confidential information. This includes, but is not limited to, contacts made through professional networking platforms such as LinkedIn, where those contacts have been established or maintained in your capacity as a councillor, member of staff or other authorised user. All such contacts will be considered council property and may be subject to disclosure upon request.

9.1.5 Note that the council may, from time to time, monitor external postings on social media sites. Any employee who has a profile (for example on WhatsApp, LinkedIn or Facebook) must not misrepresent themselves or their role with the council. Councillors, staff and other authorised users are also advised that social media sites are not an appropriate place to air council concerns or complaints. These should be raised with the council or formally through the grievance procedure.

9.1.6 It is important to note that the contact details of external stakeholders and information remain the property of the council. In addition, councillors, staff and other authorised users leaving the council will be required to delete all council-related data including external stakeholders' contact details from any personal device/equipment.

10. Misuse

Misuse of IT systems and equipment is not in line with the council's standards of conduct and will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including disciplinary proceedings or in serious cases, dismissal.

11. Important notice

This is an example of a policy designed for a small council adhering to statutory minimum requirements and does not constitute legal advice. As with all policies it should be consistent with your terms and conditions of employment.

This document was commissioned by the National Association of Local Councils (NALC) for the purpose of its member councils and county associations. Every effort has been made to ensure that the contents of this document are correct at time of publication. NALC cannot accept responsibility for errors, omissions and changes to information subsequent to publication.

This document has been written by Worknest HR – a company that provides HR advice and guidance to town and parish Councils. Please contact them on 01403 240 205 for information about their services.